

AGGREGATED AUTHENTICATED IDENTITY APPARATUS FOR AND METHOD THEREFOR

TECHNICAL FIELD

The present invention relates in general to data processing systems, and in particular, to user authentication and access in a data processing system.

5

BACKGROUND INFORMATION

Many applications and operating systems (especially in a multi-user environment) support security mechanisms which include some form of user authentication. Typically a user authenticates (that is, "logs on") to the application or operating system. The application or operating system then creates a security context. A security context is a representation of the user's identity as well as any authorization information associated therewith. For example, the context may include the user's identifier (user ID), the user's role, and group membership. Once logged on, the information associated with the security context is used by the application or operating system to determine whether the user has the proper authority to access requested resources or take selected actions.

10

15

By way of example, consider a user accessing a "secure" website, using a web browser. The website requests logon information from the user, typically consisting of a user ID and a password. The user supplies values for both, and the web server verifies

that the combination provided by the user is valid, and creates a security context for the user. An illustrative security context 100 is schematically depicted in FIGURE 1. In this example, security context 100 has a user ID field 102 with the value "*identitya*," a role field 104 containing the role of the user associated with *identitya*, here an Administrator denoted by the value "*Admin*," and two group fields 106A and 106B indicating that the user associated with *identitya* is a member of two groups, denoted by the values *TeamA*, and *Staff*. The browser user, now logged on, and associated with *identitya*, attempts to retrieve information from the web server. Based on the information in the security context, the web server determines whether the users request can be satisfied. If, for example the requested information can be accessed by any user in *TeamA*, then the request can be satisfied.

An application or operating system may support a sequence of logons (which, particularly in directory server applications, may be referred to as binds) without requiring the user to log off before logging on again. Additionally, an individual user may be associated with different identities (that is, user ID values) wherein a unique context is associated with each identity. Thus, for example, a System Administrator may have an identity which associates a security context in the role of System Administrator, and a second identity that associates a context with the user that includes roles as System Administrator and Printer Administrator. The access authorities available to the same user in the security context associated with the different identities need not be the same.

The application or operating system may employ one of several alternatives when creating and destroying security context. In a first alternative, when the user logs on, and a security context is created, any pre-existing security context is destroyed. When the

user logs off the security contest is destroyed. This alternative is typically used when logging into web and LDAP servers. (An artisan of ordinary skill in the art would understand that LDAP refers to the Lightweight Directory Access Protocol, which is an open industry standard for accessing a directory, which is a particular database containing information describing attributes associated with users and resources on a network. The specifications for the LDAP Version 3 may be found in Request for Comments (RFC) 2251. (RFCs are known by artisans of ordinary skill in the data processing art to be publications by which Internet standards are promulgated.) An alternative model saves a pre-existing security context by, for example, pushing the context onto a stack, and a new security context created. The new security context is used to access resources. When the user logs off, the new security context is destroyed, and the pre-existing security context is restored, that is, popped off the stack. This model is supported by, for example, the Distributed Computing Environment (DCE). (An artisan of ordinary skill in the art would recognize the DCE as a standardized architecture for distributing applications transparently across networks of computers. DCE is promulgated by the Open Software Foundation (OSF).) In both of these models, the user's access is determined by the current security context. Thus, if the user needs access that requires authority not associated with the current context, the user must log onto the system with the user's identity that corresponds to a security context that is associated with the required level of access authority. As a consequence, the security policies may typically be established in a simple hierarchical structure, whereby each level of authorization includes all of the access rights granted by the authorization levels lower in the hierarchy. This may be understood by referring to FIGURE 1B illustrating a hierarchical structure

of access authority in Venn diagram form. In the exemplary hierarchical structure in FIGURE 1B, four levels of authority are depicted. Level 108 may be associated with general user access authority. Level 110 may be associated with Printer Administrator access authority, which access authority includes all of the general user authority and additionally, authority necessary to perform the tasks associated with maintaining and configuring networked printer resources. Level 112 may correspond to the authorization level for a Network Administrator. In the hierarchical structure of FIGURE 1B, these authorities would include the authorities granted general users as well as those granted the Printer Administrator and additionally the authorities required to perform the tasks associated with the management of the network generally. Level 114 may be associated with a System Administrator, which authorities include those of the general user, the Printer and Network Administrators, and additionally the authorities necessary to perform the tasks associated with management of the overall system. Consequently, in such a structure, when say for example, the Network Administrator logs on to perform a general user operation, perhaps access to a distributed application, for example, a spreadsheet application, the Network Administrator is logged on with additional authorities not necessary to perform the current task. Such logons with authorities that are not necessary present opportunities for security breaches. Thus the hierarchical structure, of which FIGURE 1B is exemplary, is not a particularly satisfactory alternative to the problem of multiple logons and logouts. Consequently, there is a need in the art for mechanisms to permit finer granularity in access authorization structures without exacerbating the complications associated with multiple user logins.

SUMMARY OF THE INVENTION

The aforementioned needs are addressed by the present invention. Accordingly there is provided, in a first form, an authentication method. The method includes
5 generating a first security context in response to a first user authentication. A second security context is generated in response to a second user authentication. The second security context aggregates the first security context and a security context corresponding to an identity in the second user authentication.

There is also provided, in a second form, a computer program product embodied
10 in a tangible storage medium, the program product comprising a program of instructions for performing the method steps for an authentication method. Included are instructions for generating a first security context in response to a first user authentication. The instructions also perform the step of generating a second security context in response to a second user authentication, in which the second security context aggregates the first
15 security context and a security context corresponding to an identity in the second user authentication.

Additionally, there is provided, in a third form, a data processing system including circuitry operable for generating a first security context in response to a first user authentication and circuitry operable for generating a second security context in
20 response to a second user authentication. The second security context aggregates the first security context and a security context corresponding to an identity in the second user authentication.

The foregoing has outlined rather broadly the features and technical advantages

of the present invention in order that the detailed description of the invention that follows may be better understood. Additional features and advantages of the invention will be described hereinafter which form the subject of the claims of the invention.

11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60
61
62
63
64
65
66
67
68
69
70
71
72
73
74
75
76
77
78
79
80
81
82
83
84
85
86
87
88
89
90
91
92
93
94
95
96
97
98
99
100
101
102
103
104
105
106
107
108
109
110
111
112
113
114
115
116
117
118
119
120
121
122
123
124
125
126
127
128
129
130
131
132
133
134
135
136
137
138
139
140
141
142
143
144
145
146
147
148
149
150
151
152
153
154
155
156
157
158
159
160
161
162
163
164
165
166
167
168
169
170
171
172
173
174
175
176
177
178
179
180
181
182
183
184
185
186
187
188
189
190
191
192
193
194
195
196
197
198
199
200
201
202
203
204
205
206
207
208
209
210
211
212
213
214
215
216
217
218
219
220
221
222
223
224
225
226
227
228
229
230
231
232
233
234
235
236
237
238
239
240
241
242
243
244
245
246
247
248
249
250
251
252
253
254
255
256
257
258
259
260
261
262
263
264
265
266
267
268
269
270
271
272
273
274
275
276
277
278
279
280
281
282
283
284
285
286
287
288
289
290
291
292
293
294
295
296
297
298
299
300
301
302
303
304
305
306
307
308
309
310
311
312
313
314
315
316
317
318
319
320
321
322
323
324
325
326
327
328
329
330
331
332
333
334
335
336
337
338
339
340
341
342
343
344
345
346
347
348
349
350
351
352
353
354
355
356
357
358
359
360
361
362
363
364
365
366
367
368
369
370
371
372
373
374
375
376
377
378
379
380
381
382
383
384
385
386
387
388
389
390
391
392
393
394
395
396
397
398
399
400
401
402
403
404
405
406
407
408
409
410
411
412
413
414
415
416
417
418
419
420
421
422
423
424
425
426
427
428
429
430
431
432
433
434
435
436
437
438
439
440
441
442
443
444
445
446
447
448
449
450
451
452
453
454
455
456
457
458
459
460
461
462
463
464
465
466
467
468
469
470
471
472
473
474
475
476
477
478
479
480
481
482
483
484
485
486
487
488
489
490
491
492
493
494
495
496
497
498
499
500
501
502
503
504
505
506
507
508
509
510
511
512
513
514
515
516
517
518
519
520
521
522
523
524
525
526
527
528
529
530
531
532
533
534
535
536
537
538
539
540
541
542
543
544
545
546
547
548
549
550
551
552
553
554
555
556
557
558
559
560
561
562
563
564
565
566
567
568
569
570
571
572
573
574
575
576
577
578
579
580
581
582
583
584
585
586
587
588
589
590
591
592
593
594
595
596
597
598
599
600
601
602
603
604
605
606
607
608
609
610
611
612
613
614
615
616
617
618
619
620
621
622
623
624
625
626
627
628
629
630
631
632
633
634
635
636
637
638
639
640
641
642
643
644
645
646
647
648
649
650
651
652
653
654
655
656
657
658
659
660
661
662
663
664
665
666
667
668
669
670
671
672
673
674
675
676
677
678
679
680
681
682
683
684
685
686
687
688
689
690
691
692
693
694
695
696
697
698
699
700
701
702
703
704
705
706
707
708
709
710
711
712
713
714
715
716
717
718
719
720
721
722
723
724
725
726
727
728
729
730
731
732
733
734
735
736
737
738
739
740
741
742
743
744
745
746
747
748
749
750
751
752
753
754
755
756
757
758
759
760
761
762
763
764
765
766
767
768
769
770
771
772
773
774
775
776
777
778
779
780
781
782
783
784
785
786
787
788
789
790
791
792
793
794
795
796
797
798
799
800
801
802
803
804
805
806
807
808
809
810
811
812
813
814
815
816
817
818
819
820
821
822
823
824
825
826
827
828
829
830
831
832
833
834
835
836
837
838
839
840
841
842
843
844
845
846
847
848
849
850
851
852
853
854
855
856
857
858
859
860
861
862
863
864
865
866
867
868
869
870
871
872
873
874
875
876
877
878
879
880
881
882
883
884
885
886
887
888
889
890
891
892
893
894
895
896
897
898
899
900
901
902
903
904
905
906
907
908
909
910
911
912
913
914
915
916
917
918
919
920
921
922
923
924
925
926
927
928
929
930
931
932
933
934
935
936
937
938
939
940
941
942
943
944
945
946
947
948
949
950
951
952
953
954
955
956
957
958
959
960
961
962
963
964
965
966
967
968
969
970
971
972
973
974
975
976
977
978
979
980
981
982
983
984
985
986
987
988
989
990
991
992
993
994
995
996
997
998
999
1000
1001
1002
1003
1004
1005
1006
1007
1008
1009
1010
1011
1012
1013
1014
1015
1016
1017
1018
1019
1020
1021
1022
1023
1024
1025
1026
1027
1028
1029
1030
1031
1032
1033
1034
1035
1036
1037
1038
1039
1040
1041
1042
1043
1044
1045
1046
1047
1048
1049
1050
1051
1052
1053
1054
1055
1056
1057
1058
1059
1060
1061
1062
1063
1064
1065
1066
1067
1068
1069
1070
1071
1072
1073
1074
1075
1076
1077
1078
1079
1080
1081
1082
1083
1084
1085
1086
1087
1088
1089
1090
1091
1092
1093
1094
1095
1096
1097
1098
1099
1100
1101
1102
1103
1104
1105
1106
1107
1108
1109
1110
1111
1112
1113
1114
1115
1116
1117
1118
1119
1120
1121
1122
1123
1124
1125
1126
1127
1128
1129
1130
1131
1132
1133
1134
1135
1136
1137
1138
1139
1140
1141
1142
1143
1144
1145
1146
1147
1148
1149
1150
1151
1152
1153
1154
1155
1156
1157
1158
1159
1160
1161
1162
1163
1164
1165
1166
1167
1168
1169
1170
1171
1172
1173
1174
1175
1176
1177
1178
1179
1180
1181
1182
1183
1184
1185
1186
1187
1188
1189
1190
1191
1192
1193
1194
1195
1196
1197
1198
1199
1200
1201
1202
1203
1204
1205
1206
1207
1208
1209
1210
1211
1212
1213
1214
1215
1216
1217
1218
1219
1220
1221
1222
1223
1224
1225
1226
1227
1228
1229
1230
1231
1232
1233
1234
1235
1236
1237
1238
1239
1240
1241
1242
1243
1244
1245
1246
1247
1248
1249
1250
1251
1252
1253
1254
1255
1256
1257
1258
1259
1260
1261
1262
1263
1264
1265
1266
1267
1268
1269
1270
1271
1272
1273
1274
1275
1276
1277
1278
1279
1280
1281
1282
1283
1284
1285
1286
1287
1288
1289
1290
1291
1292
1293
1294
1295
1296
1297
1298
1299
1300
1301
1302
1303
1304
1305
1306
1307
1308
1309
1310
1311
1312
1313
1314
1315
1316
1317
1318
1319
1320
1321
1322
1323
1324
1325
1326
1327
1328
1329
1330
1331
1332
1333
1334
1335
1336
1337
1338
1339
1340
1341
1342
1343
1344
1345
1346
1347
1348
1349
1350
1351
1352
1353
1354
1355
1356
1357
1358
1359
1360
1361
1362
1363
1364
1365
1366
1367
1368
1369
1370
1371
1372
1373
1374
1375
1376
1377
1378
1379
1380
1381
1382
1383
1384
1385
1386
1387
1388
1389
1390
1391
1392
1393
1394
1395
1396
1397
1398
1399
1400
1401
1402
1403
1404
1405
1406
1407
1408
1409
1410
1411
1412
1413
1414
1415
1416
1417
1418
1419
1420
1421
1422
1423
1424
1425
1426
1427
1428
1429
1430
1431
1432
1433
1434
1435
1436
1437
1438
1439
1440
1441
1442
1443
1444
1445
1446
1447
1448
1449
1450
1451
1452
1453
1454
1455
1456
1457
1458
1459
1460
1461
1462
1463
1464
1465
1466
1467
1468
1469
1470
1471
1472
1473
1474
1475
1476
1477
1478
1479
1480
1481
1482
1483
1484
1485
1486
1487
1488
1489
1490
1491
1492
1493
1494
1495
1496
1497
1498
1499
1500
1501
1502
1503
1504
1505
1506
1507
1508
1509
1510
1511
1512
1513
1514
1515
1516
1517
1518
1519
1520
1521
1522
1523
1524
1525
1526
1527
1528
1529
1530
1531
1532
1533
1534
1535
1536
1537
1538
1539
1540
1541
1542
1543
1544
1545
1546
1547
1548
1549
1550
1551
1552
1553
1554
1555
1556
1557
1558
1559
1560
1561
1562
1563
1564
1565
1566
1567
1568
1569
1570
1571
1572
1573
1574
1575
1576
1577
1578
1579
1580
1581
1582
1583
1584
1585
1586
1587
1588
1589
1590
1591
1592
1593
1594
1595
1596
1597
1598
1599
1600
1601
1602
1603
1604
1605
1606
1607
1608
1609
1610
1611
1612
1613
1614
1615
1616
1617
1618
1619
1620
1621
1622
1623
1624
1625
1626
1627
1628
1629
1630
1631
1632
1633
1634
1635
1636
1637
1638
1639
1640
1641
1642
1643
1644
1645
1646
1647
1648
1649
1650
1651
1652
1653
1654
1655
1656
1657
1658
1659
1660
1661
1662
1663
1664
1665
1666
1667
1668
1669
1670
1671
1672
1673
1674
1675
1676
1677
1678
1679
1680
1681
1682
1683
1684
1685
1686
1687
1688
1689
1690
1691
1692
1693
1694
1695
1696
1697
1698
1699
1700
1701
1702
1703
1704
1705
1706
1707
1708
1709
1710
1711
1712
1713
1714
1715
1716
1717
1718
1719
1720
1721
1722
1723
1724
1725
1726
1727
1728
1729
1730
1731
1732
1733
1734
1735
1736
1737
1738
1739
1740
1741
1742
1743
1744
1745
1746
1747
1748
1749
1750
1751
1752
1753
1754
1755
1756
1757
1758
1759
1760
1761
1762
1763
1764
1765
1766
1767
1768
1769
1770
1771
1772
1773
1774
1775
1776
1777
1778
1779
1780
1781
1782
1783
1784
1785
1786
1787
1788
1789
1790
1791
1792
1793
1794
1795
1796
1797
1798
1799
1800
1801
1802
1803
1804
1805
1806
1807
1808
1809
1810
1811
1812
1813
1814
1815
1816
1817
1818
1819
1820
1821
1822
1823
1824
1825
1826
1827
1828
1829
1830
1831
1832
1833
1834
1835
1836
1837
1838
1839
1840
1841
1842
1843
1844
1845
1846
1847
1848
1849
1850
1851
1852
1853
1854
1855
1856
1857
1858
1859
1860
1861
1862
1863
1864
1865
1866
1867
1868
1869
1870
1871
1872
1873
1874
1875
1876
1877
1878
1879
1880
1881
1882
1883
1884
1885
1886
1887
1888
1889
1890
1891
1892
1893
1894
1895
1896
1897
1898
1899
1900
1901
1902
1903
1904
1905
1906
1907
1908
1909
1910
1911
1912
1913
1914
1915
1916
1917
1918
1919
1920
1921
1922
1923
1924
1925
1926
1927
1928
1929
1930
1931
1932
1933
1934
1935
1936
1937
1938
1939
1940
1941
1942
1943
1944
1945
1946
1947
1948
1949
1950
1951
1952
1953
1954
1955
1956
1957
1958
1959
1960
1961
1962
1963
1964
1965
1966
1967
1968
1969
1970
1971
1972
1973
1974
1975
1976
1977
1978
1979
1980
1981
1982
1983
1984
1985
1986
1987
1988
1989
1990
1991
1992
1993
1994
1995
1996
1997
1998
1999
2000
2001
2002
2003
2004
2005
2006
2007
2008
2009
2010
2011
2012
2013
2014
2015
2016
2017
2018
2019
2020
2021
2022
2023
2024
2025
2026
2027
2028
2029
2030
2031
2032
2033
2034
2035
2036
2037
2038
2039
2040
2041
2042
2043
2044
2045
2046
2047
2048
2049
2050
2051
2052
2053
2054
2055
2056
2057
2058
2059
2060
2061
2062
2063
2064
2065
2066
2067
2068
2069
2070
2071
2072
2073
2074
2075
2076
2077
2078
2079
2080
2081
2082
2083
2084
2085
2086
2087
2088
2089
2090
2091
2092
2093
2094
2095
2096
2097
2098
2099
2100
2101
2102
2103
2104
2105
2106
2107
2108
2109
2110
2111
2112
2113
2114
2115
2116
2117
2118
2119
2120
2121
2122
2123
2124
2125
2126
2127
2128
2129
2130
2131
2132
2133
2134
2135
2136
2137
2138
2139
2140
2141
2142
2143
2144
2145
2146
2147
2148
2149
2150
2151
2152
2153
2154
2155
2156
2157
2158
2159
2160
2161
2162
2163
2164
2165
2166
2167
2168
2169
2170
2171
2172
2173
2174
2175
2176
2177
2178
2179
2180
2181
2182
2183
2184
2185
2186
2187
2188
2189
2190
2191
2192
2193
2194
2195
2196
2197
2198
2199
2200
2201
2202
2203
2204
2205
2206
2207
2208
2209
2210
2211
2212
2213
2214
2215
2216
2217
2218
2219
2220
2221
2222
2223
2224
2

BRIEF DESCRIPTION OF THE DRAWINGS

For a more complete understanding of the present invention, and the advantages thereof, reference is now made to the following descriptions taken in conjunction with the accompanying drawings, in which:

FIGURE 1A schematically illustrates a security context which may be used in an embodiment of the present invention;

FIGURE 1B illustrates in Venn diagram form, a hierarchical access authorization structure;

FIGURE 2 illustrates, in block diagram form, a data processing system implemented in accordance with an embodiment of the present invention;

FIGURE 3 illustrates, in flow chart form, a methodology in accordance with an embodiment of the present invention;

FIGURE 4 schematically illustrates additional security context to which may be used in an embodiment of the present invention; and

FIGURE 5 illustrates in Venn diagram form, a partitioning of access authority which may be used in an embodiment of the present invention.

DETAILED DESCRIPTION

The present invention provides a system and method for aggregating authenticated identities. A security context created in response to a first user logon is saved in response to a second logon. A composite or aggregate security context is created based on the identity passed in the second logon. Access may then be granted (or denied) based on the current, aggregated security context. Upon logout of the user based on the second identity, the aggregate security context is destroyed, and the security context reverts to the context previously saved. Alternatively, in another embodiment, all security contexts, including those on the stack, may be destroyed.

In the following description, numerous specific details are set forth such as specific field values, etc. to provide a thorough understanding of the present invention. However, it will be obvious to those skilled in the art that the present invention may be practiced without such specific details. In other instances, well-known circuits have been shown in block diagram form in order not to obscure the present invention in unnecessary detail. For the most part, details concerning timing considerations and the like have been omitted in as much as such details are not necessary to obtain a complete understanding of the present invention and are within the skills of persons of ordinary skill in the relevant art.

Refer now to the drawings wherein depicted elements are not necessarily shown to scale and wherein like or similar elements are designated by the same reference numeral through the several views.

Referring first to FIGURE 2, an example is shown of a data processing

system 200 which may be used for the invention. The system has a central processing unit (CPU) 210, which is coupled to various other components by system bus 212. Read only memory ("ROM") 216 is coupled to the system bus 212 and includes a basic input/output system ("BIOS") that controls certain basic functions of the data processing system 200. Random access memory ("RAM") 214, I/O adapter 218, and communications adapter 234 are also coupled to the system bus 212. I/O adapter 218 may be a small computer system interface ("SCSI") adapter that communicates with a disk storage device 220. Communications adapter 234 interconnects bus 212 with an outside network enabling the data processing system to communicate with other such systems. Input/Output devices are also connected to system bus 212 via user interface adapter 222 and display adapter 236. Keyboard 224, track ball 232, mouse 226 and speakers 228 are all interconnected to bus 212 via user interface adapter 222. Display monitor 238 is connected to system bus 212 by display adapter 236. In this manner, a user is capable of inputting to the system throughout the keyboard 224, trackball 232 or mouse 226.

Preferred implementations of the invention include implementations as a computer system programmed to execute the method or methods described herein, and as a computer program product. According to the computer system implementation, sets of instructions for executing the method or methods are resident in the random access memory 214 of one or more computer systems configured generally as described above. Until required by the computer system, the set of instructions may be stored as a computer program product in another computer memory, for example, in disk drive 220 (which may include a removable memory such as an optical disk or floppy disk for

eventual use in the disk drive 220). Further, the computer program product can also be stored at another computer and transmitted when desired to the user's work station by a network or by an external network such as the Internet. One skilled in the art would appreciate that the physical storage of the sets of instructions physically changes the medium upon which it is stored so that the medium carries computer readable information. The change may be electrical, magnetic, chemical, biological, or some other physical change. While it is convenient to describe the invention in terms of instructions, symbols, characters, or the like, the reader should remember that all of these and similar terms should be associated with the appropriate physical elements.

Note that the invention may describe terms such as comparing, validating, selecting, identifying, or other terms that could be associated with a human operator. However, for at least a number of the operations described herein which form part of at least one of the embodiments, no action by a human operator is desirable. The operations described are, in large part, machine operations processing electrical signals to generate other electrical signals.

Refer now to FIGURE 3, illustrating, in flow chart form, authentication methodology 300 in accordance with the principles of the present invention. In step 302 it is determined if a user authentication has been received, that is if a user has requested a logon by submitting a user ID value and password value. (The submission of a user ID value and password may simply be referred to as submitting a user ID and password hereinbelow, however, the values will be referred to explicitly where the context requires.)

If a user authentication has been received, in step 304 it is determined if security

context aggregation is enabled. Aggregation may be enabled for a application/operating system in response to a predetermined set of policies. For example, if the policies permit the user to select the type of authentication, in an embodiment of system 200, FIGURE 2, in which the operating system employs a graphical user interface (GUI), a dialog box may be presented displaying the fields for receiving the corresponding values: User ID, Password, and Aggregate identities? (Yes/No). Alternatively in an embodiment of system 100 using a command line interface (CLI), a command line "switch" may be used. Such a logon might have the exemplary form: "logon user = fred pw = foo -a" to log on with the identity "fred", with the password "foo" and the switch "-a" indicating that the logon should be aggregated. If, however, aggregation is not enabled, in step 306 a current security context, if a current security context exists, is destroyed, and in step 308 a new security context created. Based on the security context created in step 306, access is granted or denied, step 309.

Returning to step 304, if aggregation is enabled step 304 proceeds by the "Yes" branch. In step 310 the current security context is saved. For example, the current security context may be saved by pushing the current context onto a stack. In step 312, the current security context is aggregated with a new security context based on the identity received as the value of the user ID in step 302, and the aggregate current security context becomes the new security context. In step 309 access is granted or denied in response to the new current security context from step 312. Process 300, then proceeds loops over steps 302 and 314-16 logouts and authentications as discussed further below.

This may be further understood by referring to FIGURE 4, illustrating in

schematic form, a security context 400. Assuming that, by way of example, the user has authenticated, in step 302, FIGURE 3, with a userID of "*identityb*," and the security context associated therewith is security context 400. Field 402 contains the userID of *identityb*, the role corresponding therewith, field 404 is Printer Administrator ("*PrintAdmin*"), and the group, field 406, is "*Maintenance*." Suppose, further, that the current security context corresponds to security context 100, FIGURE 1. Then, in step 310, security context 100 is saved. Additionally, in step 312, the new security context becomes the aggregate of security context 100, FIGURE 1 and security context 400, FIGURE 4. FIGURE 4 also schematically illustrates security context 450A, which may be the new security context. Field 452 contains the userID of *identityb*. The roles associated with security context 450A is field 454 with subfields 454A and 454B, respectively, *Admin* and *PrintAdmin*. similarly, security context 450 includes field 456 containing the groups *TeamA*, subfield 456A, *Staff*, subfield 456B and *Maintenance*, subfield 456C. Alternatively, in an embodiment in which the Access Control Model of the application or operating system supports the use of individual userIDs on Access Control Lists, the user's identities may also be aggregated. (An Access Control List includes a list of entities that are to be protected, for example, file directories, etc., and an associated list of permissions.) A security context 450B corresponding to such an embodiment is also schematically illustrated in FIGURE 4. Field 452 of security context 450B has a subfields 452A and 452B containing *identitya* and *identityb*, respectively. (It would be understood by artisans of ordinary skill that security context 100, FIGURE 1 and security contexts 400 and 450, FIGURE 4, are for illustrative purposes only, and the principles of the present invention are applicable to security contexts having other,

structural implementations and values contained in the fields therein.)

Returning to step 302, if a user authentication is not received, step 302 proceeds by the "No" branch to step 314. In step 314, it is determined if the user logs out. If not, methodology 300 loops between steps 314 and 302 to receive user authentication requests, or logout requests.

Returning to step 314, if a logout is received, step 314 proceeds by the "Yes" branch, and in step 316 the current security context is destroyed. (An artisan of ordinary skill would understand that a security context may be "destroyed" by releasing, or freeing, the data structures maintaining the state of the security context, that is, freeing the portion of memory, such as RAM 214, FIGURE 2, containing the data structures.) In step 318, if aggregation has not been enabled, as discussed in conjunction with step 304, process 300 returns to step 302. Otherwise, step 318 proceeds via the "Yes" branch to step 320, and the security context saved in step 310 is reverted to. Process 300 then returns to step 302.

This may be understood by considering further the example discussed in conjunction with steps 310 and 312, FIGURE 3. Upon logoff of the user in the context of *identityb*, via step 314, the current context, security context 450, FIGURE 4 is destroyed, via step 316, FIGURE 3, and the previous context, saved via step 310, FIGURE 3, is reverted to, by for example, popping the context off of a stack, via step 320 and the "Yes" branch of step 318.

In this way an authentication mechanism is implemented which permits a user to selectively authenticate without necessarily giving up already established access. (Note that a user need not refer to a "human" user but may, for example, include a proxy server

running under a user's identity.) Consequently, access authorizations may be have fine granularity, both vertically, that is, along organizational lines, and horizontally, that is, along functional lines, to reduce the opportunity for comprise of system security without increasing the inconvenience of multiple logon/logoff sequences. Moreover, the partitioning of access authority need not be hierarchical, such as that illustrated in Venn diagram form in FIGURE 1B. Thus, for example, a Printer Administrator may have authorities not granted a System Administrator, wherein, the authorities may be disjoint, as illustrated in Venn diagram form in FIGURE 5, in which the set 502 (which may represent the set of System Administrator access authorities) does not include access authorities in set 504 (which may represent the set of System Administrator access authorities). Additionally, authorities may be partially disjoint, such a sets of authorities 506 and 508, FIGURE 5. By way or example, a System Administrator may be granted access to private personnel records, only for the purpose of backing up lost records due to a system failure, (which may, for example, be associated with a security context with a role of *Admin* and group of *Maintenance*) while a Human Resources Administrator may have access to not only back up records, but have access for reading and writing, generally. In the Venn diagram of FIGURE 5, the common authority to back up lost records, would be associated with the intersection 510 of sets 506 and 508.

Although the present invention and its advantages have been described in detail, it should be understood that various changes, substitutions and alterations can be made herein without departing from the spirit and scope of the invention as defined by the appended claims.